REMARKS

This amendment responds to the Final Office Action dated February 24, 2006 and the Advisory Action dated June 9, 2006 and the allowance of the parent case Serial No. 09/916,397, filed July 27, 2001. Claims 1, 29, 47, 72 and 73 are amended to delete "a" from the phrase "a corresponding a plurality of security levels" which deletion corrects a typographic error. Claims 72 and 73 have been amended to conform to the allowable subject matter in the parent case. The change to the specification corrects a typographic error in the priority claim. A Supplemental Declaration is filed herewith.

In the Office Action on pages 2-8, paragraphs 3-8, the patent examiner rejects claims 1-73 as being non-patentable in view of certain prior art disclosed in the following references:

U.S. Patent No.5,960,080 to Fahlman
U.S. Patent No.5,581,682 to Anderson et al.
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses
FOLDOC (URL webpage)
Schneier (Applied Cryptography)

In the Office Action, the examiner also issued a double patenting rejection based upon Serial Nos. 09/916,397 (now allowed); 10/008,218; 10/155,525; 10/155,192; 10/277,196; and 10/390,807. Applicant submits, under protest, a Terminal Disclaimer for the allowed parent case, Serial No. 09/916,397 and requests that the Examiner withdraw the double patenting rejection based upon Serial Nos. 10/008,218; 10/155,525; 10/155,192; 10/277,196; and 10/390,807 since those cases will not issue before the present case. Further, the enclosed Terminal Disclaimer linked to the Parent Case Serial Nos. 09/916,397 (now allowed) will limit the term of the present case to be coextensive

with the Parent Case and therefore the present case could never be longer in duration compared to the "sibling" cases, 10/008,218; 10/155,525; 10/155,192; 10/277,196; and 10/390,807.

> If a "provisional" nonstatutory obviousness-type double patenting (ODP) rejection is the only rejection remaining in the earlier filed of the two pending applications, while the later-filed application is rejectable on other grounds, the examiner should withdraw that rejection and permit the earlier-filed application to issue as a patent without a terminal disclaimer.

MPEP 804 (I)(B)(1), p. 800-17.

> The filing of a terminal disclaimer to obviate a rejection based on nonstatutory double patenting is not an admission of the propriety of the rejection. *Quad Environmental Technologies Corp. v. Union Sanitary District*, 946 F.2d 870, 20 USPQ2d 1392 (Fed. Cir. 1991). The court indicated that the "filing of a terminal disclaimer simply serves the statutory function of removing the rejection of double patenting, and raises neither a presumption nor estoppel on the merits of the rejection."

MPEP 804.02(II), p. 800-32.

Applicant is submitting this terminal disclaimer for the parent case in order to expedite prosecution. Applicant disagrees that the Examiner adequately explained the link or combination of the present claims with those claims in one or more of Serial Nos. 10/008,218; 10/155,525; 10/155,192; 10/277,196; and 10/390,807 with the cited prior art.

> Since the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection, the factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are employed when making an obvious-type double patenting analysis. These factual inquiries are summarized as follows: (A) Determine the scope and content of a patent claim relative to a claim in the application at issue; (B) Determine the differences between the scope and content of the patent claim as determined in (A) and the claim in the application at issue; (C) Determine the level of ordinary skill in the pertinent art; and (D) Evaluate any objective indicia of nonobviousness.
>
> The conclusion of obviousness-type double patenting is made in light of these factual determinations. Any obviousness-type double patenting rejection should make clear: (A) The differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and (B) The reasons why a person of ordinary skill in the art would conclude that the invention

> defined in the claim at issue would have been< an obvious variation of the invention defined in a claim in the patent.

MPEP § 804(II)(B)(1) p. 800-21

It is respectfully submitted that the Examiner accept the enclosed Terminal Disclaimer and withdraw the double patenting rejection with respect to Serial Nos. 10/008,218; 10/155,525; 10/155,192; 10/277,196; and 10/390,807.

The presently claimed invention is patentable because it is drawn to a "multi-level security" system and process and such system and process is patentable and distinct over the cited references. In this case, independent claims 1, 29, 47, 72 and 73 refer to "respective extract stores" in the preamble of the claims and to "storing said subsets of extracted data and said remainder data in said respective extract stores and said remainder store, respectively." See claim 1. It is respectfully submitted that claims 1, 29, 47, 72 and 73 include the concept that various levels of secret data are stored in "respective extract stores" and this is essentially the same as multiple levels of security with multiple levels of secure storage. Claim 73 provides for decrypting from many extract stores based predetermined security clearances and states: "decrypting all or portions of said data from said extract stores and remainder store with multiple level encryption only in the presence of a respective predetermined security clearance of said plurality of security levels."

In summary, Kirshenbaum '298, Lamm '907 and/or Fahlman '080 do not show, teach or suggest multiple extractions of security sensitive words related to each of a plurality of security levels, and separate storage of those security sensitive words in different secured locations for each security level (multiple extract stores), and the requirement that the user input a password ("security clearance") for each security level. Details of this analysis are set forth in the previously filed amendment.

Further in summary, Fahlman '080, Andersen '682 and Flyntz '542 do not show, teach or suggest multiple extractions of security sensitive words into a respective plurality of memory stores for each security level (extract stores). Falman '080 does not disclose nor discuss multiple security level storage and retrieval. Anderson '682 describes storing all secure data in a single document (not multiple security storage locations, one for each security level) and Flyntz '542 does not discuss STORING and RETRIEVING different security words from different extract or security memory locations.

Kirshenbaum '298 does not show separate storage of secured data, separate and apart from unsecured data. Both secured and non-secured data is stored in a single database 14. Col. 3, lines 40-44; col. 5, lines 7-10 ("The data set is stored in a database ... the document comprises secure portion and non-secure portions"); col. 5, lines 36-37 ("to retrieve those secure and non-secure portions of the document and to send the retrieved portions of the document to the output device.").

Fahlman '080 does not show, teach or suggest a remainder store for non-secured data, multiple security levels, multiple extraction of security data, storage of multiple levels, presentment of different security codes at each security level. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

Lamm '907 stores and has multiple copies of all secret-secured data about the consumer in three (3) different computers, to wit, consumer computer 12 (see legends FIG. 2, consumer computer 20, col. 5, line 48), billing - processor computer 26 (see col. 13, line 5) and enrollment server 21 (see col. 9, line 42). The three computers in Lamm '907 provide an integrated bill payment system which cannot be deconstructed into operable components. In contrast, the present invention extracts secured data, for multiple security levels, and then stores the extracted data in extract stores.

Lamm's process of storing secret data in three computers is completely different than the claimed system of storing secret data in multiple, extract stores for respective security levels.

Kluttz '161 does not show, teach or suggest multi-level extract stores nor permitting reconstruction of said data via said extract data stores only in the presence of predetermined security clearances. Kluttz '161 shows utilizing multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

With respect to **Schneier's book (Applied Cryptography)**, Schneier does not show, teach or suggest multi-level extract stores nor predetermined security clearances, nor reconstruction of said data via multiple extract stores only in the presence of said predetermined security clearances. Schneier discusses encryption and key destruction.

U.S. Patent No. 5,036,315 to **Gurley** does not cure the defects identified above with respect to Lamm '907 and the differences with respect to the present invention. Gurley does not show, teach or suggest (a) filtering data; (b) utilizing multiple extract stores and a remainder store; (c) multiple security clearances for the extract stores; and (d) permitting reconstruction of said data via the multiple extract stores only in the presence of predetermined security clearances. Gurley '315 discusses a video display control which accepts and processes two (2) video signals, one displayed in a defined window of the second video display.

Flyntz' 572 does not show, teach, or suggest the claimed (i) "filtering data input ... to obtain subsets of extracted data;" (ii) "storing said subsets of extracted data ... in respective extract stores;"

and (iii) permitting reconstruction of "some or all of said data via one or more of said respective extract stores ... only in the presence of a predetermined security clearance of said plurality of security clearances." Claim 1. See also, claim 29, 47, 72 (includes encrypting) and 73 (includes encrypting and decrypting).

Flyntz '542 is principally interested in retrieving data but the retrieval of data always occurs with a double key system, the first key required is the user's smart card; and the second key required is a mechanical cam switch associated with a removable hard drive containing all complete versions of the secured documents for that security level. Only one memory store at a time is subject to access in Flyntz '542. If the security level on the user's smart card does not match the security level of the removable hard drive, the user is only permitted to retrieve and view unclassified data. Therefore, if the user's smart card has a high level of security rating (secret "S"), and the operable hard drive is designated Classified "C", the user is not permitted access to the C data on the hard drive even though the user's security level is a higher S rating compared with the security code on the hard drive C. Further, in every implementation of the Flyntz '542 patent, if this one to one correspondence (smart card security level must be equal hard drive security level) is NO, the user is only permitted access to the unclassified (U/C) data.

In every instance, Flyntz '542 requires that the smart card used by the user must match the security code of the hard drive (U/C; S; CL) and if not, the user is only permitted to see unclassified data U/C 24. An important feature of the Flyntz '542 system is that the data is on a removable hard drive. Col. 2, line 26 (herein "2/26"); 3/5; 3/31, 5/66; 7/30; 7/35; 7/38; 8/55; 9/41; 10/49; 11/33 ("if the nth memory device were detected by the (n-1)th sensor switch); 11/65; 12/4; 12/30; 12/40; 12/61; 13/15; 13/18; 13/37; 13/67. As explained in detail throughout Flyntz '542, the insertion of

this removable hard drive (S or CL) closes a mechanical switch, such as a cam, and the closure of the S or CL drive cam, when matched to the S or CL security level on a smart card of a user, permits the user to access only the secured data on the inserted hard drive and not other data on any other hard drive. Flyntz '542 discusses the required matching between the security level on the user's smart card with the security level on the inserted hard drive memory (S or CL) at the following locations. Col. 2, line 40; Col. 3, lines 28-32; 3/36; 4/2; 5/66; 6/53; 7/30; 8/54; 8/63; 9/55; 10/1; 10/34; 10/49; 11/46; 11/64; 12/39; 12/59; 11/66.

Anderson '682 does not show, teach or suggest storing extract data in respective extract stores in one or more computers and Anderson '682 also does not show, teach or suggest "permitting reconstruction of some or all of said data via one or more of said subsets of extracted data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels." Claim 1.

Anderson '682 shows that the security information is stored in a single document. For example, looking at the illustrations in Anderson '682, FIG. 2B shows a document and shows a data stream representing that document (see the bottom of the page, rectangular box with five segments including "begin page"). FIG. 3B shows an insert in the document "we should get a better map" which is not shown in the original document FIG. 2B and the added information "we should get a better map" is identified in the "object overlay" shown at the bottom of FIG. 3B after "begin page." FIG. 4 shows another insert in the original document "this needs a nice color picture." In the text of Anderson '682, the disclosure identifies that the document would include triplets (col. 3, line 65, herein "3/65") and theses triplets are shown in the table at 4/11 and include the length of triplet, the type of conditional overlay (normal, annotation or redaction) and the level of the overlay. "The level triplet is compared to one contained within the application being invoked and, if it is equal or lower

than the application level, the overlay is processed. Otherwise, the overlay is not performed." 4/37.

In applying the Anderson '682 system to a security item, the disclosure states:

> Returning to the decision block 4, if the overlay is a redaction, the system pursues to decision block 8. In decision block 8, the system examines the security level of the redaction and compares it to the security level of the user, which is already known to the system, if the redaction security level exceeds that of the user, the system determines that the user does not have ability to view the documents prior to redaction .

5/3.

Further, Anderson '682 specifically states "at this point, the system returns to block one in order to process any additional overlays that may be found in the current page of the document." Therefore, it is clear that the secure information or secure data in Anderson '682 is included in a single document and that secured data is stored with the document on the computer system. Therefore, Anderson '682 does not show, teach or suggest storing said extracted data in "said respective extract stores" which is a required step in claim 1, and also does not show, teach or suggest "permitting reconstruction of some or all of said data via one or more of said subsets of extracted data and remainder data only in the presence of a predetermined security clearance of said plurality of security levels." Claim 1.

The **FOLDOC** (URL webpage) reference does not discuss multi-level security system claimed herein.

Moses '950 relates to a dynamic digital filter using a neural network to adjust a digital filter for decoding an audio input signal and for reconstructing a digitized audio signal. The neural network determines whether periodic or aperiodic signals are present and then adjusts the coefficients of the filter. Multi-level security systems are not discussed in Moses '950.

Applicant respectfully requests that the examiner approve the patentability of claims 1 - 73.

Respectfully submitted,

By /Robert Kain/
Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Fort Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being filed via efiling with Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on June 28, 2006.

/Robert Kain/
Robert C. Kain, Jr.
Reg. No. 30,648

\\TIGER\Data Share\RCK\CLIENTS\Redlich\Patents\6851-02cip1-amdt-3d-062806.wpd